7Ш

УДК 004.415.24

***І.В. Швідченко***
Інститут кібернетики імені В.М. Глушкова НАН України
Україна, пр. Академіка Глушкова, 40, 03680, МСП, Київ-187

# Про один метод стеганографічного аналізу контейнерів-зображень

***I.V. Shvidchenko***
Glushkov Institute of Cybernetic of National Academy of Sciences of Ukraine
Ukraine, Kyiv-187, 40, Glushkov Ave., 03680

# *On a Method for Cover Images Steganalysis*

***И.В. Швидченко***
Институт кибернетики имени В.М. Глушкова НАН Украины
Украина, пр. Академика Глушкова, 40, 03680, МСП, Киев-187

# Об одном методе стеганографического анализа контейнеров-изображений

Наведено аналіз стеганографічного методу заміни найменш значущого біту. Розглянуто і досліджено метод стеганоаналізу «Sample pairs analysis», який дозволяє оцінити відносну довжину повідомлення в випадку застосування алгоритму розподіленого вкраплення інформації в контейнер-зображення. Проведено тестування даного методу.
**Ключові слова:** захист інформації, стеганографія, стеганоаналіз, Sample Pairs Analysis, прихована передача даних, контейнер, повідомлення.

Steganographic method of replacing the least significant bits is analyzed. A method of steganalysis «Sample pairs analysis», which allows to estimate the relative length of the message, in the case of a random algorithm of information embedding in a cover image is considered and investigated. Testing of this method has been carried out.
**Key words:** information protection, steganography, steganalysis, Sample Pairs Analysis, hidden data transfer, cover, message.

Проанализирован стеганографический метод замены наименее значимого бита. Рассмотрен и исследован метод стеганографического анализа «Sample pairs analysis», который позволяет оценить относительную длину сообщения в случае применения алгоритма распределенного внедрения информации в контейнер-изображение. Проведено тестирование данного метода.
**Ключевые слова:** защита информации, стеганография, стеганоанализ, Sample Pairs Analysis, скрытая передача данных, контейнер, сообщение.

## Вступ

На сьогодні в мережі Інтернет можна знайти безліч безкоштовного або умовно-безкоштовного програмного забезпечення зі стеганографії. Алгоритми, які покладені в основу таких програм, виконують вкраплення конфіденційного повідомлення в так звані контейнери (зображення, аудіо-, відео-). Використання подібних програм дає змогу непомітно для сторонніх осіб передавати по відкритим каналам зв’язку будь-яку закриту інформацію одночасно з відкритою (видимою) інформацією, що не має конфіденційного характеру. Непомітність такої передачі даних може бути вико рис-тана для реалізації злочинних намірів. Запобігти несанкціонованій передачі інформації

методами стеганографії дозволяє стеганоаналіз. Основна задача стеганоаналізу – встановлення факту існування в контейнері прихованої інформації. Взагалі, виявлення прихованої передачі даних, прихованих одним із багатьох існуючих методів стеганографії в різні формати контейнерів є досить складним процесом. Наприклад, використання широко відомого методу стеганоаналізу на основі критерію $\chi^2$ (хі-квадрат) дозволяє отримати гарні результати, якщо вкраплення інформації здійснювалось методом послідовної заміні найменш значущих біт елементів контейнера-зображення або методом вкраплення з заповненням, однак цей метод не спрацьовує коли відбувається псевдовипадковий вибір молодших біт (розподілене вкраплення). Щоб отримати більш достовірну відповідь про наявність додаткової інформації в потенційному контейнері необхідно мати комплекс стеганоаналітичних методів.

**Метою даної роботи** є дослідження стеганоаналітичного методу «Sample pairs analysis», що дозволяє виміряти довжини прихованих повідомлень, які вкраплюються в випадковому порядку у молодші значущі біти природних напівтонових зображень.

# Аналіз методу заміни найменш значущого біту

Метод заміни найменш значущого біту (НЗБ) є найпростішим (класичним) методом, який використовується у стеганографії. Метод полягає в наступному. В якості вихідного контейнера застосовується зображення значення пікселів якого лежать в діапазоні [0, 255] (наприклад, зображення в відтінках сірого або колірна складова растрового зображення у режимі True Color). Метод НЗБ замінює молодший значущий біт кожного значення піксела в зображенні відповідним бітом повідомлення, яке приховується. Парне значення піксела зображення або зберігає своє значення, або збільшується на одиницю. При цьому, воно ніколи не зменшується. Для непарного значення піксела навпаки. Відповідно до цього визначення можна сформувати так звані пари НЗБ значень пікселів як множину $\{(0\,1),(2\,3),(4\,5),\ldots\}$. Операція вкраплення має таку властивість: кожне значення піксела залишається у своїй НЗБ парі після вкраплення. Наприклад, після вкраплення біту у піксель із кольором 2, значення піксела завжди буде залишатися в тій самій НЗБ парі $(2\,3)$. Також і з іншими значеннями.

Надалі, припустимо, що маємо 8-бітові напівтонові зображення (grayscale images) і позначимо $T_C[i]$ кількість пікселів у пустому зображенні з кольором $i$, і так само $T_S[i]$ для стеганозображення. Назвемо $T_C$ типовим зразком зображення $C$. Типовий зразок це ненормована гістограма. Використовуючи цю систему позначень, і властивість пар НЗБ, можна записати

$$T_C[2i]+T_C[2i+1]=T_S[2i]+T_S[2i+1]\ \forall i=0\ldots127\,. \tag{1}$$

Це означає, що кількість пікселів у кожній парі НЗБ пустого зображення й стеганозображення однакова, тому що жоден піксель не може бути вилучений із цієї пари в процесі вкраплення. Ця сума зберігається для довільної відносної довжини повідомлення $q$.

Щоб показати перший аспект цієї схеми вкраплення, розглянемо повідомлення $m$ як випадкову послідовність $\{0,1\}$. Припустимо, що повідомлення вкраплюється з відносною довжиною $q$ (визначимо її як $q=m/n$, де $m$ – довжина повідомлення

в бітах, $n$ – загальна кількість пікселів в зображенні). Тоді, усереднена гістограма $T_S$ стеганозображення може бути виражена в такий спосіб:

$$T_S[2i] = (1-q)T_C[2i] + \frac{q}{2}T_C[2i] + \frac{q}{2}T_C[2i+1] \ , \qquad (2)$$

$$T_S[2i+1] = (1-q)T_C[2i+1] + \frac{q}{2}T_C[2i] + \frac{q}{2}T_C[2i+1] \ , \qquad (3)$$

для кожної пари гістограми $i = 0,...,127$. Ці рівняння одержуються, використовуючи наступну ідею (рис. 1). Коли вкраплюється повідомлення з відносною довжиною повідомлення $q$, відношення $1-q$ всіх пікселів з кольором $2i$ не змінюється, але обробляється його порція $q$.

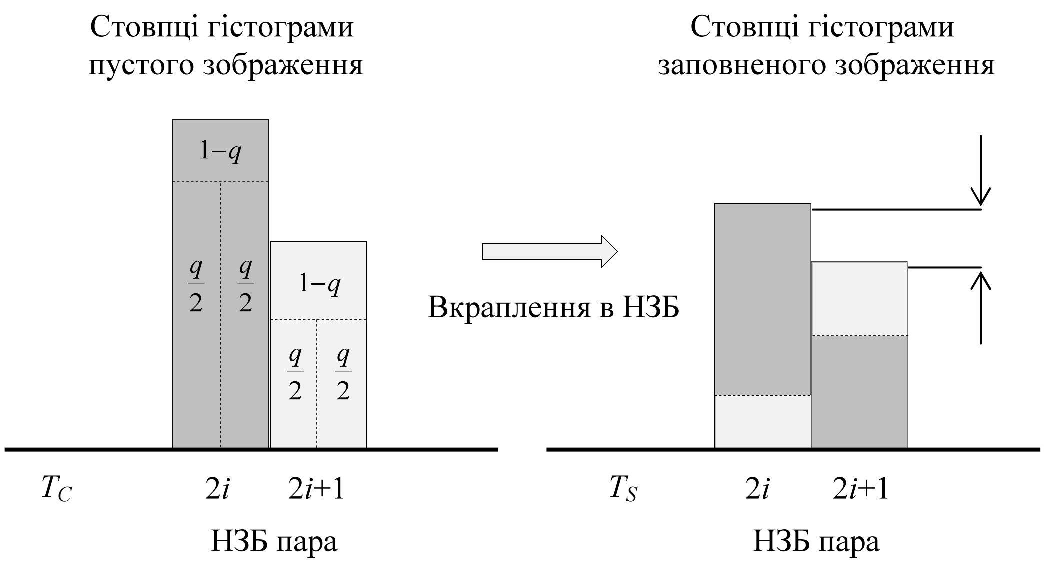



Рисунок 1 – Вплив вкраплення в НЗБ на пари стовпчиків гістограми

Завдяки цій обробці маємо рівну ймовірність (повідомлення – потік двійкових даних), з огляду на піксель із парним НЗБ $\left(\frac{q}{2}T_C[2i]\right)$, що не змінюється, і з непарним НЗБ, що змінюється на протилежний з $2i$ на $2i+1$. Так само і для випадку з кольором $2i+1$. Окремий випадок цих рівнянь відбувається для повністю вкрапленого зображення, де $q=1$. У цьому випадку, алгоритм вкраплення в НЗБ повністю вирівнює всі стовпчики гістограми стеганозображення.

Зміну типу стовпчиків гістограми можна побачити на рис. 2, де зображений типовий зразок оригінального зображення і типовий зразок повністю заповненого зображення.

Процес вирівнювання стовпчиків гістограми для кожної пари НЗБ не є природним для цифрових зображень, і отже, це є артефактом, що викликаний вкрапленням у НЗБ. Можна використати цей артефакт і виміряти розбіжність між кожним стовпцем, але це не буде надійним методом.

Однак цей артефакт можна використати, щоб одержати верхню границю для відносної довжини повідомлення $q$. Припустимо, що $T_S[2i] > T_S[2i+1]$, обчислимо $T_S[2i] - T_S[2i+1]$, використовуючи рівняння (2) та (3).

Маємо

$$T_S[2i]-T_S[2i+1]=(1-q)(T_C[2i]-T_C[2i+1])\le(1-q)(T_C[2i]+T_C[2i+1])$$

і при цьому, використовуючи (1), одержимо

$$q\le\frac{2T_S[2i+1]}{T_S[2i]+T_S[2i+1]}.$$

Те ж саме можна зробити для випадку $T_S[2i]<T_S[2i+1]$, і в результаті одержимо наступну верхню границю

$$q\le 2\frac{\min\{T_S[2i],T_S[2i+1]\}}{T_S[2i]+T_S[2i+1]}.$$

Типовий зразок порожнього контейнера | Типовий зразок заповненого контейнера

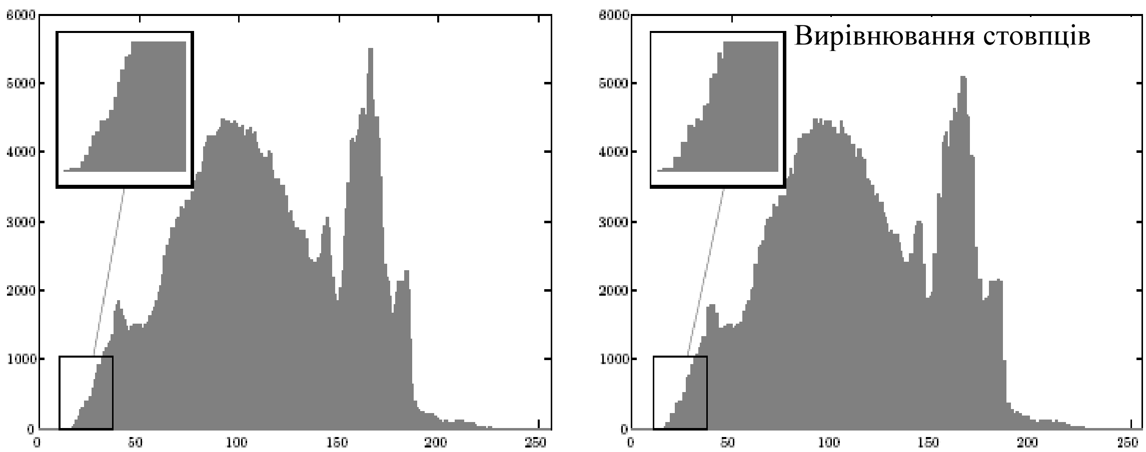



Рисунок 2 – Порівняння типових зразків пустого й повністю заповненого зображення

Метод стеганоаналізу, який використовує аналіз гістограми, отриманої по елементах зображення, і оцінку розподілу пар значень цієї гістограми, називається методом на основі критерію $\chi^2$ (хі-квадрат).

Однак цей метод не спрацьовує, коли відбувається псевдовипадковий вибір молодших бітів (розподілене вкраплення).

Взагалі, методи стеганоаналізу, які використовують статистичні характеристики першого порядку (гістограми) ігнорують залежність між сусідніми пікселами природних зображень.

Більш надійні й точні алгоритми виявлення повідомлення ті, які використовують просторові залежності (кореляцію) в зображеннях.

Прикладом такого методу є метод «Sample pairs analysis», запропонований авторами робіт [1-4].

# Метод «Sample pairs analysis»

Поділимо зображення на пари сусідніх пікселів (горизонтально суміжних) і позначимо цю пару $(u,v)\in \mathsf{P}$, де $\mathsf{P}$ – множина всіх пар пікселів у зображенні. Розмір множини $\mathsf{P}$ дорівнює $\frac{n}{2}$, де $n$ – кількість пікселів.

Далі, поділимо множину $\mathsf{P}$ на три неперетинні підмножини $\mathsf{P} = \chi \cup \mathsf{Y} \cup \mathsf{Z}$, де

$$\begin{aligned} \chi &= \{(u,v) \in \mathsf{P} | (v \text{ парне і } u < v) \text{ або } (v \text{ непарне і } u > v)\} \\ \mathsf{Y} &= \{(u,v) \in \mathsf{P} | (v \text{ непарне і } u < v) \text{ або } (v \text{ парне і } u > v)\}. \\ \mathsf{Z} &= \{(u,v) \in \mathsf{P} | u = v\} \end{aligned} \quad (4)$$

Поділимо множину $\gamma$ на дві підмножини $\mathcal{V}$ та $\mathcal{W}$ ($\mathcal{Y} = \mathcal{V} \cup \mathcal{W}$), де $\mathcal{V} = \mathcal{Y} - \mathcal{W}$, і

$$\begin{aligned} \mathcal{W} &= \{(u,v) \in \mathcal{P} | (u,v) = (2k, 2k+1) \text{ або } (u,v) = (2k+1, 2k)\} \\ \mathcal{V} &= \{(u,v) \in \mathcal{P} | (u,v) \notin \mathcal{W}\}. \end{aligned} \quad (5)$$

Множини $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{W}$, $\mathcal{V}$, $\mathcal{Z}$ назвемо вихідними множинами. Відмітимо, що $\mathcal{P} = \mathcal{X} \cup \mathcal{W} \cup \mathcal{V} \cup \mathcal{Z}$.

Проаналізуємо, що відбувається, коли повідомлення вкраплюється в останній бітовий зріз піксельних значень.

Вкраплення, змінюючи НЗБ, змінює значення деяких пікселів. Отже, відносне упорядкування деяких пар пікселів в $\mathcal{P}$, які підлеглі вкрапленню, буде змінено. Для пари пікселів $(u,v)$ можливі чотири ситуації:

а) обидва значення $u$ й $v$ залишаються незміненими (зразок модифікації 00);

б) тільки $u$ змінюється (зразок модифікації 10);

в) тільки $v$ змінюється (зразок модифікації 01);

г) і $u$, і $v$ змінюються (зразок модифікації 11).

Якщо перебуваємо в ситуації «а» (б, в, г), говоримо, що зразок модифікації через вкраплення в НЗБ дорівнює 00 (10, 01, 11, відповідно).

Процес вкраплення приводить до зміни приналежності деяких пар пікселів між вихідними множинами (рис. 3).

На рис. 3 кожна стрілка, яка намальована від множини $A$ до множини $B$, і яка позначена зразком модифікації, означає, що будь-яка пара пікселів множини $A$ стає парою пікселів множини $B$, якщо модифікується зазначеним зразком під час вкраплення в НЗБ.

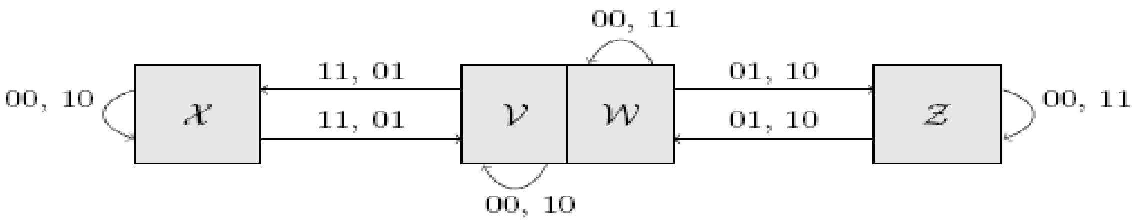



Рисунок 3 – Діаграма переходів між вихідними множинами при використанні методу вкраплення в НЗБ

Для кожного зразка модифікації $\pi \in \{00, 10, 01, 11\}$ й будь-якої підмножини $A \subseteq \mathcal{P}$, позначимо $\rho(\pi, A)$ відносну кількість пар пікселів в $A$, що модифіковані зразком $\pi$.

Якщо біти повідомлення розсіюються в довільному порядку по зображенню і таким чином незалежні від змісту зображення (не адаптивне вкраплення), тоді для кожного зразка модифікації $\pi \in \{00, 10, 01, 11\}$ і кожної вихідної множини $A \subseteq \mathcal{P}$, $A \in \{\mathcal{X}, \mathcal{V}, \mathcal{W}, \mathcal{Z}\}$ повинно бути

$$\rho(\pi, A) = \rho(\pi, \mathcal{P}). \quad (6)$$

Якщо $q$ – відносна довжина повідомлення (довжина вкрапленого повідомлення в бітах поділена на загальну кількість пікселів $q = m/n$), тоді очікувана відносна кількість модифікованих НЗБ вкрапленням пікселів дорівнює $\frac{q}{2}$. Використовуючи рівняння (6), маємо

а) $\rho(00, \mathcal{P}) = \left(1 - \frac{q}{2}\right)^2$;

б) $\rho(01, \mathcal{P}) = \rho(10, \mathcal{P}) = \frac{q}{2}\left(1 - \frac{q}{2}\right)$;

в) $\rho(11, \mathcal{P}) = \left(\frac{q}{2}\right)^2$.

Ці ймовірності переходу й множина перехідних зв'язків з рис. 3 дозволяють виразити кількість елементів вихідних множин після вкраплення як функції від $q$ та кількості елементів множини перед вкрапленням.

Для кожної $A \in \{\mathcal{X}, \mathcal{Y}, \mathcal{V}, \mathcal{W}, \mathcal{Z}\}$, позначимо $A'$ множину, яка визначається в такий же спосіб як множина $A$, але розглядаючи значення пікселів після вкраплення. Тоді одержуємо наступні рівняння:

$$|\mathcal{X}'| = |\mathcal{X}|\left(1 - \frac{q}{2}\right) + |\mathcal{V}|\frac{q}{2} \tag{7}$$

$$|\mathcal{V}'| = |\mathcal{V}|\left(1 - \frac{q}{2}\right) + |\mathcal{X}|\frac{q}{2} \tag{8}$$

$$|\mathcal{W}'| = |\mathcal{W}|\left(1 - q + \frac{q^2}{2}\right) + |\mathcal{Z}|q\left(1 - \frac{q}{2}\right). \tag{9}$$

Мета полягає в тому, щоб одержати рівняння для невідомої величини $q$, використовуючи тільки кількість елементів вихідних множин, оскільки вони можуть бути обчислені безпосередньо зі стеганозображення.

Однак, щоб усунути невідомі елементи вихідних множин контейнера-зображення, маємо потребу в додатковому рівнянні. Відзначимо, що в середньому

$$|\mathcal{X}| = |\mathcal{Y}|. \tag{10}$$

Це припущення вірно для природних зображень, які, як правило, містять певну кількість шуму, тому що він в однаковій мірі має $u > v$ або $u < v$ незалежно від того, чи є $u$ парним або непарним.

Рівняння (7) і (8) означають, що

$$|\mathcal{X}'| - |\mathcal{V}'| = (|\mathcal{X}| - |\mathcal{V}|)(1 - q) \tag{11}$$

У такий спосіб у силу того, що $|\mathcal{X}| = |\mathcal{Y}|$, маємо $|\mathcal{X}| = |\mathcal{V}| + |\mathcal{W}|$, і з рівняння (11) маємо

$$|\mathcal{X}'| - |\mathcal{V}'| = |\mathcal{W}|(1 - q). \tag{12}$$

З рис. 3 видно, що процес вкраплення не змінює множини $\mathcal{W} \cup \mathcal{Z}$. Позначивши $\gamma = |\mathsf{W}| + |Z| = |\mathsf{W}'| + |Z'|$, і замінивши $|\mathcal{Z}|$ на $\gamma - |\mathcal{W}|$, рівняння (9) стає

$$|\mathcal{W}'| = |\mathcal{W}|\left(1 - q + \frac{q^2}{2}\right) + |\mathcal{Z}|q\left(1 - \frac{q}{2}\right) = |\mathcal{W}|\left(1 - q + \frac{q^2}{2}\right) + (\gamma - |\mathcal{W}|)q\left(1 - \frac{q}{2}\right) = \\ = |\mathcal{W}|(1-q)^2 + \gamma \cdot q\left(1 - \frac{q}{2}\right). \quad (13)$$

Вилучення $|\mathcal{W}|$ з (12) і (13) приводить до

$$|\mathcal{W}'| = (|\mathcal{X}'| - |\mathcal{V}'|)\cdot(1-q) + \gamma \cdot q\left(1 - \frac{q}{2}\right). \quad (14)$$

Так як $|\mathcal{X}'| + |\mathcal{V}'| + |\mathcal{W}'| + |\mathcal{Z}'| = |\mathcal{P}|$, рівняння (14) еквівалентно

$$\frac{\gamma}{2}q^2 + (2|\mathcal{X}'| - |\mathcal{P}|)q + |\mathcal{Y}'| - |\mathcal{X}'| = 0. \quad (15)$$

Відзначимо, що $\mathcal{X}', \mathcal{Y}', \mathcal{W}', \mathcal{Z}'$ можуть бути обчислені зі стеганозображення ($\gamma = |\mathcal{W}'| + |\mathcal{Z}'|$). Невідома довжина вкрапленого повідомлення $q$ є менше рішення квадратного рівняння (15), за умови, що $\gamma \neq 0$. Якщо в рівняння є два корені комплексно сполученого числа, тоді повинні бути взяті тільки їх дійсні частини. Крім того, якщо менший корінь від'ємний, може бути тільки один результат $q = 0$, оскільки відомо, що $q$ не повинна бути від'ємною.

Якщо $\gamma = 0$, то (15) стає тотожно рівним незалежно від $q$, і отже цей метод стеганоаналізу перестає працювати. Дійсно, коли $\gamma = 0$, це означає, що $|\mathcal{X}'| = |\mathcal{X}| = |\mathcal{Y}| = |\mathcal{Y}'| = \frac{|\mathcal{P}|}{2}$. Оскільки $\gamma = |\mathcal{W}| + |\mathcal{Z}|$, можна побачити з визначень вихідних множин, що $\gamma$ є числом пар пікселів в $\mathcal{P}$, які відрізняються тільки за молодшим значущим бітом. Для природних зображень імовірність нульового $\gamma$ є дуже малою.

Метод «Sample Pairs Analysis» був надалі оптимізований в [1], [2], [5], [6] і розширений на групи більш ніж двох пікселів в [7], [8], даючи ще більш точну й достовірну продуктивність, спеціально для коротких повідомлень.

# Результати тестування методу «Sample Pairs Analysis»

Для тестування роботи методу «Sample Pairs Analysis» була обрана база даних з 1000 зображень в форматі *.pgm (напівтонові (portable graymap) – 8 біт на піксель) розміром $512 \times 512$ [9].

Створено 2 бази даних.

**І база даних**. За допомогою Matlab програми, яка виконує приховання псевдовипадковим методом в усі контейнери була вкраплена інформація з різною довжиною повідомлення – 5, 20, 50% від об'єму контейнера. Таким чином, сформовано 3 набори стеганоконтейнерів на яких було проведено тестування. За допомогою Matlab коду виконана перевірка роботи методу «Sample Pairs Analysis». На рис. 4 зображений розподіл передбачуваної довжини повідомлення для пустих контейнерів і для трьох наборів стеганоконтейнерів. Середню передбачувану довжину повідомлення $\overline{q} = \frac{\sum_{i=1}^{1000} q_i}{1000}$ і її середньоквадратичне відхилення $\sigma = \sqrt{\frac{1}{1000}\sum_{i=1}^{1000}(q_i - \overline{q})^2}$ наведено в табл. 1.

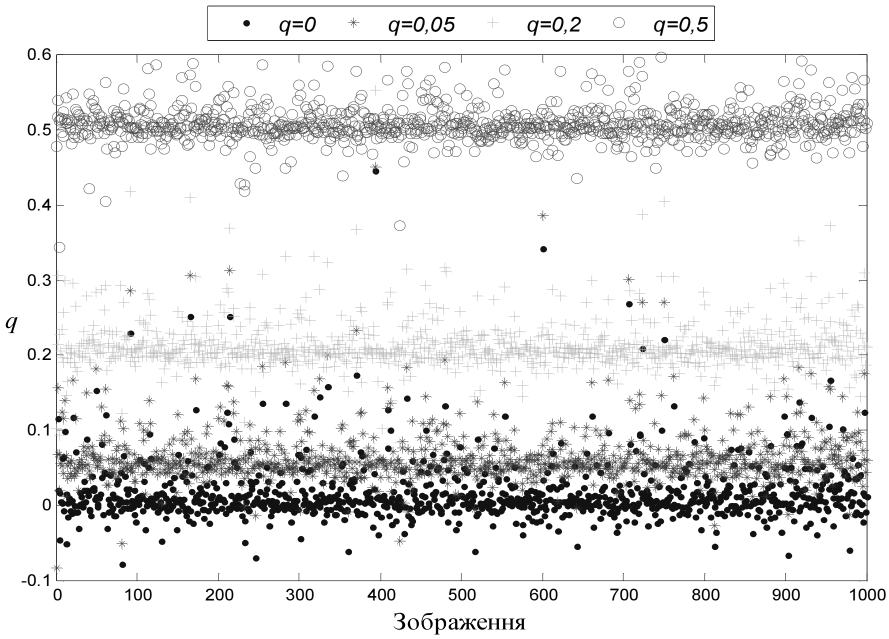



Рисунок 4 – Оцінка відносної довжини повідомлення для напівтонових *.pgm зображень з прихованою інформацією методом розподіленого вкраплення

Таблиця 1 – Середньоквадратичне відхилення $\sigma = \sqrt{\frac{1}{1000}\sum_{i=1}^{1000}\left(q_i - \overline{q}\right)^2}$

| Пустий контейнер | $q = 0{,}05$ | $q = 0{,}2$ | $q = 0{,}5$ |
|---|---|---|---|
| 0,0153± 0,0376 | 0,0645±0,0381 | 0,2139±0,0365 | 0,5089±0,0265 |

**ІІ база даних**. Сформовано три набори стеганоконтейнерів, використовуючи стеганографічний метод ±1 вкраплення, який є оптимізованою версією методу НЗБ. Замість заміни найменшого біту зображення відповідним бітом повідомлення, відповідне значення піксела збільшується або зменшується у випадковому порядку тоді, коли значення НЗБ має бути зміненим. ±1 вкраплення описується наступним чином:

$$s_i = \begin{cases} c_i + 1, & \text{якщо} \quad m \neq \text{НЗБ}(c_i) \text{ і } (\eta > 0 \text{ або } c_i = 0) \\ c_i - 1, & \text{якщо} \quad m \neq \text{НЗБ}(c_i) \text{ і } (\eta < 0 \text{ або } c_i = 255), \\ c_i, & \text{якщо} \quad m = \text{НЗБ}(c_i) \end{cases} \tag{16}$$

де $\eta$ є незалежною і однаково розподіленою випадковою змінною з рівномірним розподілом в діапазоні $\{-1,+1\}$, а $c_i$ і $s_i$ є відповідно значеннями пікселів контейнера і стеганоконтейнера. Інформація була вкраплена в контейнери з довжиною повідомлення – 5, 20, 50% від об’єму контейнера. Результати тестування наведені на рис. 5.

В табл. 2 наведено середню передбачувану довжину повідомлення і її середньоквадратичне відхилення.

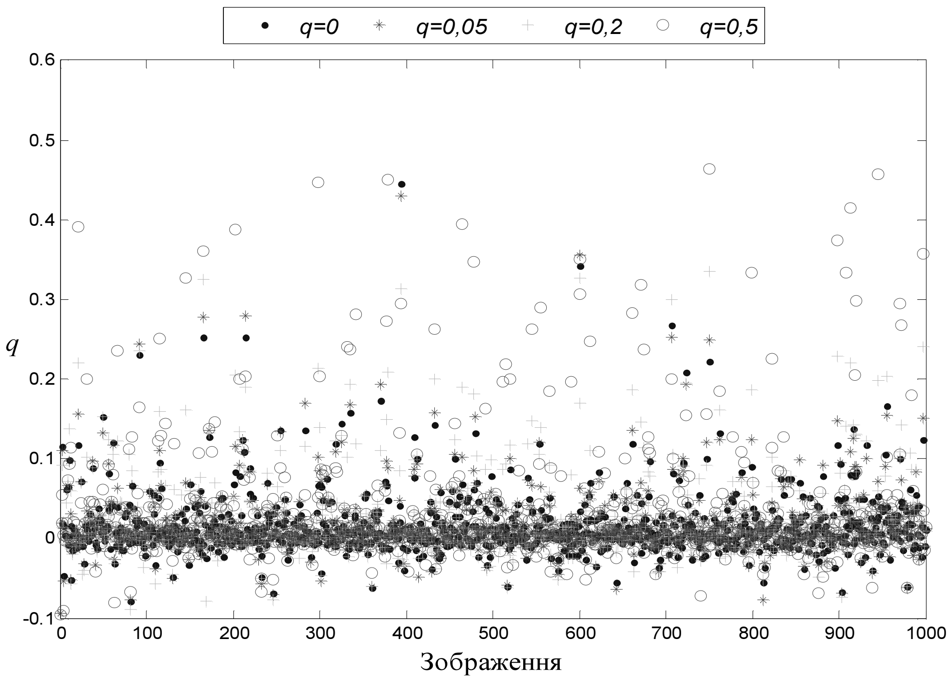



Рисунок 5 – Оцінка відносної довжини повідомлення для *.pgm зображень з вкрапленою інформацією методом ±1 вкраплення

Таблиця 2 – Середня передбачувана довжина повідомлення і її середньоквадратичне відхилення

| Пустий контейнер | $q$ = 0,05 | $q$ = 0,2 | $q$ = 0,5 |
|---|---|---|---|
| 0,0153± 0,0376 | 0,0168±0,0390 | 0,0197±0,0456 | 0,0266±0,0666 |

Як видно з результатів, метод дозволяє добре оцінити відносну довжину повідомлення для *.pgm зображень у випадку застосування методу розподіленого вкраплення.

У методі ±1 вкраплення усунута асиметрія, яка присутня в класичному методі. При такому підході створюються статистичні зміни, які дозволяють виявити відмінність між заповненим і пустим контейнером, однак, вони є незначними, і відсоток їх виявлення значно нижчий ніж для класичного методу НЗБ.

Метод «Sample Pairs Analysis» при застосуванні методу ±1 вкраплення не спрацьовує (рис. 5). Виявлення інформації, прихованої таким методом, потребує більш «витончених» стеганоаналітичних методів.

# Висновки

Розглянутий метод «Sample Pairs Analysis», який використовується для оцінки відносної довжини повідомлення, в випадку застосування алгоритму вкраплення в НЗБ. Цей метод використовує аналіз операції вкраплення (стеганоалгоритму) і визначає кількість артефактів, створених у процесі вкраплення, іншими словами, оцінює кількість біт прихованих у зображенні.

# Література

1. Dumitrescu S. Detection of LSB steganography via sample pair analysis / S. Dumitrescu, X. Wu, Z. Wang // Information Hiding, 5th International Workshop. – 2003. – Vol. 2578. – P. 355-372.

2. Lu P. An improved sample pairs method for detection of LSB embedding / P. Lu, X. Luo, Q. Tang, L. Shen // Information Hiding, 6th International Workshop. – 2004. – Vol. 3200. – P. 116-127.
3. Dumitrescu S. On steganalysis of random LSB embedding in continuous-tone images / S. Dumitrescu, X. Wu, and N. Memon // Proceedings ICIP. – 2002. – P. 324-339.
4. Fridrich J. Detecting LSB steganography in color and grayscale images / J. Fridrich, M. Goljan, R. Du // IEEE Multimedia, Special Issue on Security. – 2001. – Vol. 8. – P. 22-28.
5. Ker A. Quantitative evaluation of pairs and RS steganalysis / A. Ker // Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. – 2004. – Vol. 5306. – P. 83-97.
6. Ker A. Improved detection of LSB steganography in grayscale images / A. Ker. // Preproceedings, Information Hiding, 6th International Workshop. – 2005. – Vol. 3200. – P. 97-115.
7. Ker A. A general framework for structural analysis of LSB replacement / A. Ker // Proceedings 7th Information Hiding Workshop. – 2005. – Vol. 3727. – P. 276-311.
8. Dumitrescu S. LSB steganalysis based on higher-order statistics / S. Dumitrescu, X. Wu // Proceedings ACM Multimedia and Security Workshop. – 2005.
9. Break Our Steganographic System [Електронний ресурс]. – Режим доступу : http://exile.felk.cvut.cz/boss/BOSSFinal/

# Literatura

1. Dumitrescu S., Wu X., Wang Z. Detection of LSB steganography via sample pair analysis // Information Hiding, 5th International Workshop. – 2003. – Vol. 2578. – P. 355-372.
2. Lu P., Luo X., Tang Q., Shen L.. An improved sample pairs method for detection of LSB embedding // Information Hiding, 6th International Workshop. – 2004. – Vol. 3200. – P. 116-127.
3. Dumitrescu S., Wu X. and Memon N. On steganalysis of random LSB embedding in continuous-tone images // Proceedings ICIP. – 2002. – P. 324-339.
4. J. Fridrich, M. Goljan, and R. Du. Detecting LSB steganography in color and grayscale images // IEEE Multimedia, Special Issue on Security. – 2001. – Vol. 8. – P. 22-28.
5. Ker A. Quantitative evaluation of pairs and RS steganalysis // Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. – 2004. – Vol. 5306. – P. 83-97.
6. Ker A. Improved detection of LSB steganography in grayscale images // Preproceedings, Information Hiding, 6th International Workshop. – 2005. – Vol. 3200. – P. 97-115.
7. Ker A. A general framework for structural analysis of LSB replacement // Proceedings 7th Information Hiding Workshop. – 2005. – Vol. 3727. – P. 276-311.
8. Dumitrescu S., Wu X.. LSB steganalysis based on higher-order statistics // Proceedings ACM Multimedia and Security Workshop. – 2005.
9. Break Our Steganographic System. – http://exile.felk.cvut.cz/boss/BOSSFinal/

***RESUME***

***I.V. Shvidchenko***

## *On a Method for Cover Images Steganalysis*

The task of steganalysis is to establish the existence of hidden information in a cover image. The detection of hidden data transfer is a complicated process. To establish the existence of hidden information in a cover image or to confirm its absence it is needed to use complex steganalysis methods because the information can be hidden by one of the numerous steganography methods.

The article presents an analysis of replacing method of the least significant bit, which is a classical method in steganography. The steganalysis method «Sample pairs analysis», which allows to estimate the relative length of the message, in the case of a random algorithm of information embedding in a cover image is described. The testing results of this method are presented.

*Стаття надійшла до редакції 18.04.2013*